IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. MATTHEW WILLIAM SCHWIER, Defendant.	)	No. 3:17-cr-00095-SLG

[PROPOSED] ORDER GRANTING MOTION FOR ADDITIONAL TERMS FOR ROTECTIVE ORDER

Having duly considered the United States' Motion for Additional Terms for Protective Order and Notice of Compliance with Supplemental Order (the "Motion"), the Court ~~grants the Motion and ORDERS that:~~ denies the government's motion at Doc.244 but supplements its orders at Doc.231 and 243 as follows:

~~1.~~ ~~The government will provide a computer at the Orange County Regional Computer Forensics Laboratory ("OCRCFL"), located at 3800 W. Chapman Avenue, Suite 800, Orange, CA 92868. The computer will have one version of Torrential Downpour installed, *i.e.* version 1.23, one of the versions used in this investigation.~~ The Torrential Downpour software installed will not have access to law enforcement's database of hash values from known child pornography images.

The government will provide a copy of both Torrential Downpour versions used in this case, i.e. v. 1.15 and v. 1.23 to the defense on either CD/ DVD media or USB solid state or mechanical drive at the Orange County Regional Computer Forensics Laboratory.

The government shall produce at the RCFL both versions of the TorrentialDownpour software, the government's "validation" results, and Det. Erdley's Report no later than November 20, 2019.

//

2. The only persons who will have access to the ~~computer~~ ~~are~~ software are Jeffrey Fischbach and Robert Herz (collectively "the defense"). The defense will have access to the ~~computer~~ software for ~~21 consecutive~~ thirty (30) calendar days of testing.

3. ~~The computer will contain one network card. The defense will not make any connections to this computer other than through the network card.~~

4. The defense may bring digital media, computers, and phones into the room with the ~~computer~~ software.

5. The defense will not remove the ~~computer~~ software from the OCRCFL. The defense will not copy Torrential Downpour.

6. ~~The computer will be sealed with evidence tape. Other than the network card, all other ports/connections to the computer will be sealed with evidence tape. The defense will not tamper with or open the computer, nor break or remove the evidence tape~~.

7. The defense will not download or distribute child pornography ~~using the computer~~. Any downloading of child pornography would constitute a violation of the federal criminal code.

8. ~~All communications with the Torrential Downpour computer will be preserved via Wireshark. This preservation includes all communications with the computer containing Torrential Downpour during the 21 days of testing, both communications during testing and at all times the computer is powered up. The defense shall maintain~~

the Wireshark data pending further order of the Court.

9. At the conclusion of testing, the FBI will "zip" all the Wireshark files, meaning it will use software to compress them. The FBI will "hash" the zipped file(s), burn the zipped file(s) to a disk(s), sign the disk(s), and provide the disk(s) to the defense to maintain said disk(s) until further order by the Court. Both the defense and the FBI will be provided the hash values associated with these Wireshark file(s). However, the government will not possess the disk(s) themselves. At the conclusion of this matter, the Court will order the destruction of all copies of the disks, under circumstances to be determined, in order to prevent dissemination of the data thereon.

The government may provide the computer by November 20, 2019. The government's compliance with this Order satisfies the government's obligations under United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012).

Moreover, the Court reaffirms its prior protective Order (Dkt. 231), as follows:

Defense counsel and defense expert may not disclose their notes, the information contained in the notes, or any other information relating to their observation of the Torrential Downpour validation process or subsequent forensic examination of the computers involved therein to any person other than each other. Any information, data, and notes derived from the defense's observation of the validation process or its subsequent forensic examination shall be used solely for the purpose of conducting proceedings in this case and for no other purpose whatsoever. It shall not be disseminated to any other person

without prior order of the Court.

Nothing herein shall prevent either the government or the defendant from referencing the technical specifications of the software or any other materials in connection with pleadings or motions filed in this case, provided the materials are filed under seal and/or submitted to the Court for in camera inspection.

Violation of this protective order may be punishable by contempt of court, whatever other sanction the Court deems just, and/or any other sanctions which are legally available.

DATED this _____ day of November, 2019, at Anchorage, Alaska.

_____
UNITED STATES DISTRICT COURT JUDGE